Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.

Державне управління: удосконалення та розвиток. 2025. № 4.

DOI: http://doi.org/10.32702/2307-2156.2025.4.12

УДК 343.1:341.24

А. О. Надежденко,

к. держ. упр., доцент кафедри права, Маріупольський державний університет

ORCID ID: https://orcid.org/0000-0002-1774-5952

ПРАВООХОРОННІ ОРГАНИ ЯК СУБ'ЄКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

A. Nadezhdenko,

PhD in Public Administration, Associate Professor of the Department of Law,

Mariupol State University

LAW ENFORCEMENT AGENCIES AS SUBJECTS OF ENSURING THE INFORMATION SECURITY OF THE STATE

У статті досліджено роль правоохоронних органів у забезпеченні інформаційної безпеки держави. Розглянуто нормативно-правові основи їх діяльності, особливості функціонування в умовах гібридної війни та інформаційних загроз. Проаналізовано механізми запобігання, запобігання та нейтралізації інформаційних атак, дезінформації, кіберзлочинності. Визначено ключові суб'єкти системи інформаційної безпеки, серед яких Служба безпеки України, Національна поліція, Служба зовнішньої розвідки, Офіс Генерального

прокурора, Державне бюро розслідувань та Бюро економічної безпеки. Наголошено на необхідності удосконалення міжвідомчої взаємодії та адаптації стратегій до сучасних викликів у сфері інформаційної безпеки. Дослідження акцентує увагу на важливості створення ефективної системи інформаційної безпеки, що обґрунтовується на міжвідомчій координації, використанні сучасних технологій та посиленні аналітичних спроможностей правоохоронних органів.

The article examines the role of law enforcement agencies as key actors in ensuring the information security of the State in the context of modern threats and hybrid warfare. The author identifies the main challenges facing Ukraine's national security in the information sphere, including disinformation, propaganda, cybercrime and information attacks aimed at undermining state sovereignty.

The author analyzes the legal framework governing the activities of law enforcement agencies in the field of information security, in particular, the provisions of the Law of Ukraine "On the Fundamentals of National Security of Ukraine", the Information Security Strategy of Ukraine and the Law of Ukraine "On Cybersecurity". The author analyzes the effectiveness of these acts and the need for their adaptation to modern challenges.

Particular attention is paid to the mechanisms of countering information threats, including detection, prevention and neutralization of information attacks, cybercrime, disinformation and manipulative influence on society. The role of law enforcement agencies in digital forensics, control over the information space and combating cybercrime is investigated. The importance of the introduction of modern technologies, in particular, big data analysis, artificial intelligence and blockchain solutions in the activities of law enforcement agencies is determined.

The role of interaction between governmental and non-governmental institutions in ensuring information security, including cooperation between law enforcement agencies, civil society, the private sector and international organizations, is outlined.

The key actors of the information security system of Ukraine are identified: The Security Service of Ukraine, the National Police, the Foreign Intelligence Service, the Office of the Prosecutor General, the State Bureau of Investigation, and the Bureau of Economic Security.

The author draws conclusions about the need for interagency coordination, development of cyber units, creation of specialized think tanks, and raising the level of digital literacy among the population. The author emphasizes the importance of developing a unified information security strategy, strengthening assistance to law enforcement agencies and international cooperation in countering information threats.

Ключові слова: *правоохоронні органи, інформаційна безпека, кіберзлочинність, дезінформація, гібридна війна, державна безпека*

Keywords: *law enforcement agencies, information security, cybercrime, disinformation, hybrid warfare, state security*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. В умовах сучасних глобальних та регіональних інформаційних протистоянь, деструктивних комунікативних впливів, зіткнення різновекторних національних інформаційних інтересів, поширення інформаційної експансії та агресії, захист національного інформаційного простору та забезпечення інформаційної безпеки стають пріоритетними стратегічними завданнями правоохоронних органів у системі загальної безпеки. Забезпечення інформаційного суверенітету, формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою для України, яка часто є об'єктом зовнішньої інформаційної експансії, маніпулятивних пропагандистських технологій та руйнівного інформаційного вторгнення.

В умовах сучасної гібридної війни та інтенсивного розвитку інформаційних технологій інформаційна безпека держави набуває критичного

значення. Правоохоронні органи України виступають ключовими суб'єктами забезпечення інформаційної безпеки, оскільки їхні функції охоплюють запобігання, виявлення, нейтралізацію та розслідування інформаційних загроз, у тому числі кіберзлочинності, пропаганди, дезінформації та інформаційних операцій, спрямованих на підрив державного суверенітету.

Аналіз останніх досліджень і публікацій. Вивченню питань забезпечення інформаційної безпеки держави приділялася значна увага науковців-правників, зокрема, Антонюк В. В., Гнатенко В.С., Березовська І. Р., Русак Д. М., Довгань О. Д., Ільченко О.В. Олійник О. В., Панченко О.А, Пилипчук В. Г., Федченко Д. І., Шеломенцев В. П. та ін., проте тема не є вичерпною і дослідження функціонування правоохоронних органів у галузі забезпечення інформаційної безпеки залишається актуальним.

Формулювання цілей статті (постановка завдання). Метою статті є дослідження ролі правоохоронних органів у забезпеченні інформаційної безпеки держави в умовах сучасних загроз та гібридної війни.

Виклад основного матеріалу дослідження.

Національна безпека держави суттєво залежить від забезпечення інформаційної безпеки. На підтвердження цієї тези слід навести положення Закону України «Про основи національної безпеки України». Так, державна політика у сферах національної безпеки і оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на інші її напрями (ч. 4 ст. 3) [1].

Окремо також зазначимо про такий нормативний акт як Стратегія інформаційної безпеки України, яка затверджена Указом Президента України. Стратегія інформаційної безпеки України визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері. В Стратегії визначається, що інформаційна безпека України - складова частина національної безпеки України, стан

захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [2].

Без сумніву, інформаційна безпека в Україні є однією з найважливіших складових національної безпеки, оскільки вона безпосередньо впливає на стійкість державного управління, економічну стабільність, соціальну злагоду та міжнародний імідж країни. Інформаційна безпека полягає у досягненні стану захищеності держави, суспільства та кожного громадянина від внутрішніх і зовнішніх загроз, що спрямовані на підрив державного суверенітету, територіальної цілісності, маніпулювання суспільною свідомістю, викривлення інформаційної реальності та дестабілізацію громадського порядку. Вона також передбачає створення умов для безперешкодного доступу до достовірної інформації, забезпечення інформаційних прав і свобод громадян, а також захист критичної інформаційної інфраструктури від кібератак та інших загроз.

Для ефективного захисту інформаційного простору та реалізації цих завдань необхідна чітка, злагоджена система органів, що може перебрати на себе завдання із захисту інформаційного простору. Сьогодні забезпечення інформаційної безпеки України як найважливішої функції держави реалізується за допомогою відповідної системи як органів державної влади, що діють у межах своєї компетенції, так і недержавних інституцій, які відіграють важливу роль у протидії дезінформації, сприяють розвитку медіаграмотності, аналізують

інформаційні ризики та формують стійкість суспільства до маніпулятивних інформаційних впливів.

На сьогодні забезпечення інформаційної безпеки України, як ключової функції держави, здійснюється на основі Конституції України, законів України, міжнародних зобов'язань та стратегічних документів, зокрема Стратегії інформаційної безпеки України. У зазначеній Стратегії інформаційної безпеки України [2] фіксуються такі основні суб'єкти системи забезпечення національної безпеки, як: Рада національної безпеки і оборони України (РНБО) та її робочий орган - Центру протидії дезінформації; Кабінет Міністрів України; Міністерство культури та стратегічних комунікацій України; Міністерство закордонних справ України; Міністерство оборони України, а також сили оборони в межах компетенції (Війська зв'язку та кібербезпеки Збройних Сил України; Служба безпеки України (СБУ); Розвідувальні органи України; Національна рада України з питань телебачення і радіомовлення; Державна служба спеціального зв'язку та захисту інформації України; органи державної влади та органи місцевого самоврядування; інститути громадянського суспільства тощо.

Усі ці суб'єкти взаємодіють між собою, створюючи складну багаторівневу систему забезпечення інформаційної безпеки України. Водночас кожен із них спеціалізується на вирішенні конкретних завдань відповідно до своєї компетенції, застосовуючи визначені законом адміністративно-правові форми та методи. Важливим аспектом їхньої діяльності є не лише захист від зовнішніх інформаційних загроз, але й формування стійкої національної інформаційної політики, що передбачає створення якісного інформаційного контенту, підвищення рівня критичного мислення громадян та розвиток інфраструктури кіберзахисту.

В свою чергу, правоохоронні органи є складовою частиною системи суб'єктів забезпечення інформаційної безпеки держави, які мають специфічні особливості функціонування в інформаційному середовищі.

Правоохоронні органи, як складова системи суб'єктів забезпечення інформаційної безпеки держави, виконують ключову роль у стримуванні та протидії загрозам інформаційній безпеці України. Вони здійснюють заходи з нейтралізації інформаційної агресії, зокрема спеціальних інформаційних операцій держави-агресора, спрямованих на підрив державного суверенітету та територіальної цілісності країни.

Водночас їх діяльність спрямована на забезпечення інформаційної стійкості суспільства та держави, що зумовлює забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами та заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина.

З огляду на широкий спектр завдань, які виконують правоохоронні органи у сфері інформаційної безпеки, акцентуємо увагу на аналізі діяльності ключових інституції, що здійснюють відповідні функції.

Рис.1. Правоохоронні органи як суб'єкти забезпечення інформаційної безпеки України

Джерело: Узагальнено та згруповано автором

Служба безпеки України у межах компетенції здійснює: 1) моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та Інтернету з метою виявлення загроз національній безпеці України в інформаційній сфері; 2) протидію проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуації [2].

Національна поліція України, зокрема Департамент кіберполіції Національної поліції України який є міжрегіональним територіальним органом Національної поліції України, що входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України, забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність у сфері боротьби з кіберзлочинністю: розслідуванням кіберзлочинів, незаконного розповсюдження дезінформації, боротьба з фейковими новинами, протидія шахрайству та маніпуляціям в інформаційному просторі [3].

Служби зовнішньої розвідки України концентрує свою діяльність на здійсненні розвідувальних операцій за-для забезпечення безпеки України та безпосередньому забезпеченні керівництва нашої держави актуальною розвідувальною інформацією. Поряд з цим, варто виділити підрозділ технічної розвідки, метою діяльності якого є, насамперед, здобуття інформації політичного, економічного, військово-технічного та науково-технічного характеру, що має особливу цінність для держави [4].

Офіс Генерального прокурора України, зокрема Управління протидії кримінальним правопорушенням у сфері кібербезпеки [5] здійснює: 1) процесуальне керівництво досудовим розслідуванням та підтримання публічного обвинувачення у кримінальних провадженнях, що стосуються кібербезпеки; 2) нагляд за законністю слідчих і негласних слідчих (розшукових) дій, що здійснюються оперативними підрозділами Бюро економічної безпеки

України, Національної поліції України, Служби безпеки України, Державного бюро розслідувань; 3) участь у судовому провадженні та підтримання публічного обвинувачення у кримінальних провадженнях про кримінальні правопорушення у сфері кібербезпеки, передбачені ст. 190 (вчинені шляхом незаконних операцій з використанням електронно-обчислювальної техніки), розділом XVI КК України, а також про інші кіберзлочини (комп'ютерні злочини); 4) контролює діяльність обласних прокуратур у цій сфері, організовує міжнародну правову допомогу, розробляє аналітичні матеріали та методичні рекомендації, а також забезпечує співпрацю з іншими правоохоронними органами для ефективного розслідування кіберзлочинів.

Державне бюро розслідувань (ДБР), вирішує завдання із запобігання, виявлення, припинення, розкриття і розслідування злочинів, пов'язаних із розголошенням державної таємниці, незаконним збором та розповсюдженням конфіденційної інформації, а також можливими правопорушеннями у сфері інформаційної безпеки та кібербезпеки вчинених службовими особами, які займають особливо відповідальне становище відповідно до частини першої статті 9 Закону України «Про державну службу»; особами, посади яких віднесено до першої - третьої категорій посад державної служби, суддями та працівниками правоохоронних органів; службовими особами НАБУ та САП [6].

Детективи Бюро економічної безпеки (БЕБ) здійснюють досудове розслідування таких кримінальних правопорушень (ст. 216 КПК) [7] як: незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231 КК), та розголошення комерційної, банківської таємниці або професійної таємниці на ринках капіталу та організованих товарних ринках (ст. 232 КК) та незаконне використання інсайдерської інформації (ст. 232^1 КК).

Висновки та перспективи подальших розвідок у даному напрямі. Таким чином ефективна діяльність правоохоронних органів у сфері інформаційної безпеки в умовах сучасних загроз та гібридної війни потребує

комплексного підходу, міжвідомчої координації та впровадження сучасних технологій для виявлення та нейтралізації інформаційних атак, дезінформації, кіберзлочинності. Наголошено, що ефективна протидія цим викликам можлива лише за умов належної нормативно-правової бази, міжвідомчої координації, використання сучасних технологій та активної взаємодії з громадянським суспільством і міжнародними партнерами. Визначено необхідність посилення аналітичних і технічних засобів правоохоронних органів, удосконалення механізмів виявлення та нейтралізації інформаційних загроз, а також розширення міжнародної співпраці у сфері кібербезпеки.

Перспективи подальших досліджень у цьому напрямку можуть охопити аналіз практичних аспектів застосування сучасних технологій штучного інтелекту та великих даних у сфері інформаційної безпеки, оцінку ефективності чинного законодавства та розробку пропозицій щодо його вдосконалення, а також вивчення міжнародного досвіду боротьби з інформаційними загрозами та можливостей його адаптації до українських реалій. Особлива увага має бути приділена оптимізація оперативно-розшукової діяльності, підвищенню аналітичної ефективності єдиних правоохоронних органів та формуванню стратегії інформаційної безпеки, що створює передумови для стабільного та безпечного інформаційного середовища в Україні.

Література

1. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/card/2469-19 (дата звернення: 29.01.2025).

2. Указ Президента України № 685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки». URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення 29.01.2025).

3. Департамент кіберполіції Національної поліції України: офіційний сайт. URL: https://cyberpolice.gov.ua/contacts/ (дата звернення 30.01.2025).

4. Служби зовнішньої розвідки України: офіційний сайт. URL: https://szru.gov.ua/about/struktura (дата звернення 30.01.2025).

5. Про затвердження Положення про управління протидії кримінальним правопорушенням у сфері кібербезпеки Офісу Генерального прокурора: Наказ Генерального прокурора від 08.12. 2022 № 275 (зі змінами, внесеними наказами Генерального прокурора від 18.05.2023 № 132, від 08.01.2024 № 7). URL: https://gp.gov.ua/ua/posts/polozhennya-pro-samostijni-strukturni-pidrozdili (дата звернення: 30.01.2025).

6. Про Державне бюро розслідувань: Закон України від 12.11.2015 № 794-VIII. URL: https://zakon.rada.gov.ua/laws/card/794-19 (дата звернення: 30.01.2025).

7. Кримінальний процесуальний кодекс України: Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text (дата звернення: 30.01.2025).

References

1. The Verkhovna Rada of Ukraine (2018), The Law of Ukraine “On the national security of Ukraine”, available at: https://zakon.rada.gov.ua/laws/card/2469-19 (Accessed 29 January 2025).

2. President of Ukraine (2021), Decree “On the decision of the National Security and Defense Council of Ukraine of October 15, 2021 “On the Information Security Strategy”, available at: https://zakon.rada.gov.ua/laws/show/685/2021#Text (Accessed 29 January 2025).

3. Cyber Police Department of the National Police of Ukraine: official website (2025), available at: https://cyberpolice.gov.ua/contacts/ (Accessed 30 January 2025).

4. Foreign Intelligence Service of Ukraine: official website (2025), available at: https://szru.gov.ua/about/struktura (Accessed 30 January 2025).

5. Office of the Prosecutor General of Ukraine (2022), Order “On approval of the Regulations on the management of counteraction to criminal offenses in the field of cybersecurity of the Office of the Prosecutor General”, available at: https://gp.gov.ua/ua/posts/polozhennya-pro-samostijni-strukturni-pidrozdili (Accessed 30 January 2025).

6. The Verkhovna Rada of Ukraine (2015), The Law of Ukraine “On the State Bureau of Investigation”, available at: https://zakon.rada.gov.ua/laws/card/794-19 (Accessed 30 January 2025).

7. The Verkhovna Rada of Ukraine (2012), “Criminal Procedure Code of Ukraine”, available at: https://zakon.rada.gov.ua/laws/show/4651-17#Text (Accessed 30 January 2025).

Стаття надійшла до редакції 27.03.2025 р.